PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: **WO 98/07249**

(43) International Publication Date: 19 February 1998 (19.02.98)

(21) International Application Number: PCT/US97/12840

(22) International Filing Date: 1 August 1997 (01.08.97)

(30) Priority Data:
08/694,814 9 August 1996 (09.08.96) US

(71) Applicant: CALIFORNIA WIRELESS, INC. [US/US]; 618 Enos Court, Santa Clara, CA 95051 (US).

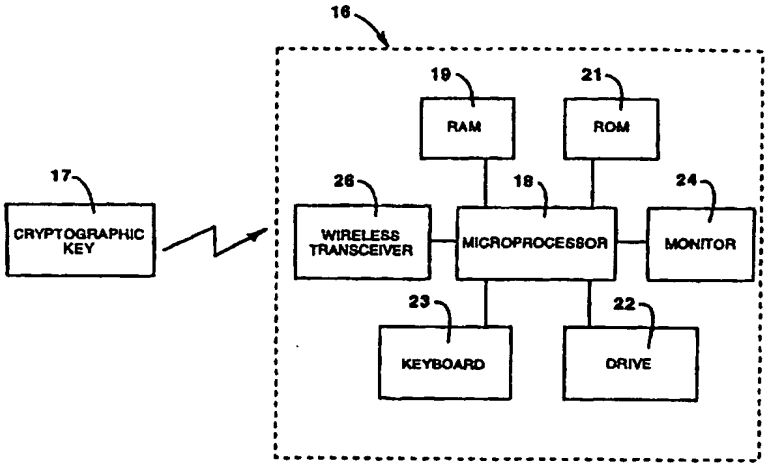
(72) Inventors: CHEPONIS, A., Michael; 618 Enos Court, Santa Clara, CA 95051 (US). RUBIN, H., Paul; 172 Marylinn Drive, Milpitas, CA 95035 (US).

(74) Agents: WRIGHT, Edward, S. et al.; Flehr, Hohbach, Test, Albritton & Herbert LLP, Suite 3400, 4 Embarcadero Center, San Francisco, CA 94111-4187 (US).

(81) Designated States: BR, CA, CN, JP, KR, MX, PL, TR, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CONTROLLED ACCESS SYSTEM AND METHOD



(57) Abstract

The system includes a cryptographic key (17) that transmits a signal to a wireless transceiver (26). The wireless transceiver (26) is connected to a microprocessor (18), a keyboard (23), a drive (22), a monitor (24), a rom (21), and a ram (19). The cryptographic key (17) transmits a wireless cryptographic signal is sent between the cryptographic key (17) and the host (16) to request authorization to use the host (16). The signal is decrypted and processed after being received to determine if access is to be granted.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

CONTROLLED ACCESS SYSTEM AND METHOD

This invention pertains generally to systems to which access is limited and, more particularly, to a system and method for controlling access to such systems.

Examples of systems to which access is limited include computers, files stored in computers, automated teller machines, and entrances to buildings. For convenience, the system to be accessed is sometimes referred to generically as the host system, or simply the host, with the understanding that it can be any type of system to which access is limited and not just the systems enumerated above.

The traditional methods of distinguishing an authorized user from an unauthorized user or imposter are by "something you have", "something you are" or "something you know". Each of these methods has its own advantages and disadvantages, and two or more of the methods can be combined.

A password is a common example of "something you know". Biometric measurement devices are one way of verifying "something you are", and physical tokens such as ordinary door keys, magnetic cards and cryptographic access devices are examples of "something you have". Each of these devices has certain limitations and disadvantages. Mechanical keys are inexpensive and reliable, but they are also easy to copy. Biometric measurement devices require elaborate specialized equipment if they are to provide high security. Cryptographic devices such as the Security Dynamics

"Secure ID" card system can require a special server, and magnetic cards require a special reader and can be copied by a "hacked" reader.

It is in general an object of the invention to provide a new and improved system and method for controlling access to a system to which access is limited.

Another object of the invention is to provide a system and method of the above character which overcome the limitations and disadvantages of techniques heretofore employed.

These and other objects are achieved in accordance with the invention by storing an encryption code in a small cryptographic key which can be carried by a person desiring access to the host, bringing the key into proximity with a wireless transceiver connected to the host, transmitting information over a wireless communication link between the host and the key, encrypting information transmitted from the key to the host in accordance with the encryption code in the key, decrypting the information received by the host, and processing the decrypted information to determine whether access to the host is authorized.

Figure 1 is block diagram of one embodiment of a controlled access system according to the invention.

Figure 2 is a block diagram of the cryptographic key in the embodiment of Figure 1.

Figure 3 is an isometric view of the cryptographic key in the embodiment of Figure 1, with the cover open and the components visible on a circuit board within the housing or case.

Figures 4 - 7 are flow charts illustrating operation of the system with different authentication and cryptographic protocols.

As illustrated in Figure 1, the system includes a host 16 and a cryptographic key 17. The host is illustrated as a computer having a microprocessor 18 with a random access memory (RAM) 19 for temporarily storing data and operating variables, a read-only memory (ROM) 21 for storing system software, a drive unit 22 for more permanent storage of software and data, a keyboard 23 and a monitor 24.

The host also includes a transceiver 26 for transferring data and other information over a wireless communications link between the computer and the cryptographic key. That link can utilize any suitable form of communication such as infrared, visible light, radio frequency or inductive coupling, and in one presently preferred embodiment, an infrared transceiver is employed. A number of computers today have infrared transceivers or ports built into them for transferring data to printers and other peripheral devices. By using a standard form of communication such as the Infrared Data Association (IrDA) Standards with those ports, secure access can be provided to existing computers without requiring any additional hardware to be added to them. The transceiver can either be an integral part of the host or it can be located remotely of the host, possibly even being connected to the host through an insecure network. In either case, the key is brought into proximity with the transceiver and actuated to exchange information with the host.

In the embodiment illustrated, the cryptographic key has generally rectangular housing or case 28 of a size which fits easily in the hand or pocket. In one present embodiment, it has a width on the order of 1-1/4 inches, a length on the order of 2 inches, and a thickness on the order of 1/2 inch. In the embodiment illustrated, it is attached to a keychain 29.

As illustrated in Figure 2, the cryptographic key includes a central processing unit (cpu) 31, a random number generator 32, RAM 33, ROM 34, non-volatile memory 36, input switches 37, and a transceiver 38. The transceiver is chosen to match the one in the host, and in the presently preferred embodiment is an IrDA-compatible infrared transceiver.

The components of the key are mounted on a circuit board 39 inside the housing or case. Those components include a microcontroller 41 which contains the microprocessor, memory and registers, a battery 42, switches 37, transceiver 38, and a light emitting diode (LED) 43 which indicates the status of the key. The infrared light source and sensor in the transceiver communicate with the host through an infrared transparent window 44 in the end wall of the housing opposite the keychain.

One relatively simple cryptographic protocol which can be employed in the invention is authentication of the user by a cryptographic variable or secret key which is shared between the cryptographic key and the host. The secret key can, for example, be a large number (e.g., 128 bits) which cannot be guessed by an attacker without an unfeasibly large, exhaustive search.

The host has a database of authorized users, which contains a user ID and a secret key for each user. As illustrated in Figure 4, the host generates a random number or cipher block R and sends that number as a challenge. The key encrypts the number R using the secret key K and sends the encrypted number CR back to the host. It also sends its user ID so that the host will know which secret key to use. The host then encrypts the number R using the secret key K and compares its result with the encrypted number CR received from the key. If the results match, the user is authenticated (*i.e.*, determined to be authorized to have access to the host), and access is permitted. If not, access is denied.

Another authentication protocol which can be utilized is hash-based authentication of the user. According to this protocol, the cryptographic key and the host both implement a secure has function H(x) such as the NIST Secure Hash Algorithm designed for use with the Digital Signature Standard (FIPS PUB 186). Numerous authentication techniques can be based on such functions.

One such technique is the S/key protocol which was designed at AT&T Bell Laboratories and is in widespread use on various computer systems. It is illustrated in Figure 5. Let HN(n,x) denote the iterated hash function, *i.e.*, the function H iterated n times. For example, HN(4,x) is the same as H(H(H(H(x)))). When a user enrolls in the system, his cryptographic key generates or is assigned a secret key K. The host stores an iterated hash of K in its database. The number of iterations is a parameter of the implementation. For 100 iterations, for example, the host initially stores HN(100,K) as the user's authentication challenge AC. It also records the number n (in this case, 100) in the database.

To authenticate a user, the host sends the number n to the cryptographic key. The cryptographic key computes the response R = HN (n-1,K) and sends that result back to the host. The host verifies that R hashes the stored authentication challenge, *i.e.*, that H(R) = AC. The host then replaces AC in its database with R and replaces n with n-1. When n reaches zero, the user must re-enroll in the system with a new K.

This approach has the advantage that the host does not need to store secret keys. Each new secret key it receives is used once, then discarded.

Another protocol which can be employed to authenticate the user is a digital signature algorithm (DSA), such as the NIST Digital Signature Algorithm described in U.S. Patent 5,231,668 and in FIPS PUB 186, the disclosures of which are incorporated herein by reference. According to that algorithm, the

cryptographic key contains a secret key KS and a corresponding public key KP, which is also a cryptographic variable. The host also stores the public key. As illustrated in Figure 6, the host generates a random number or challenge string R and transmits it to the cryptographic key. That key then generates a random "salt" string S and concatenates that string with the random number R, producing a new string R' which consists of the contents of the random number R followed by the contents of the salt string S. It also computes the digital signature DSA(R') using its secret key KP. The cryptographic key then transmits the digital signature DSA(R') to the host, along with the salt string S. The host then verifies the signature on the string R' using the public KP.

This technique is advantageous in that the cryptographic key needs to hold only one secret key, which can be used with as many hosts as desired. There is no need for concern about hosts revealing the public keys since those keys are already public. Even if the host is totally compromised, the secret component rests entirely in the cryptographic key and is still secure. The salt string prevents a potentially malicious host from gathering legitimate signatures on arbitrary strings of its own choosing.

The secret/public keys can generated be within the cryptographic key by use of a random number generator, or they can be downloaded from a secure host. Generation within the cryptographic key has the advantage that the secret key never leaves the cryptographic key, and there is no need to worry about security of a generating host.

The cryptographic key can authenticate a user either by the inputting of an identifying code (*e.g.*, a PIN) through a keypad or by other means such as a biometric sensor to scan a unique feature of the body (*e.g.*, a fingerprint or a retinal scan). If desired, the infrared transceiver in the key can be utilized to perform the scan as well as to communicate with the host.

In addition to authenticating users, the cryptographic key can also transmit a stored secret key to the host. This mode makes it convenient to access encrypted files on the host without the user having to remember or type a long password. There are several ways in which the secret key can be transmitted to the host.

One simple approach is to transmit the secret key in unencrypted form. The problem with this approach is possible interception of the transmission and capture of the secret key by eavesdroppers. With infrared systems, where the range of transmission is limited, this technique can be used in low-to-medium security applications in typical environments. However, it is probably not suitable for use in systems such as RF where the range of transmission is greater.

The protocol for the simple approach is that the host requests the secret key from the cryptographic key, and the cryptographic key sends the secret key to the host.

Another approach is to transmit the secret key in encrypted form, using a public key protocol such as Diffie-Hellman key exchange or the Hughes key transmission protocol. This avoids the security problems of the simple approach but requires a more powerful microprocessor in the cryptographic key. Diffie-Hellman key exchange is described in detail in U.S. Patent 4,200,770, the disclosure of which is incorporated herein by reference. However, its use might require the payment of license fees until the patent expires.

Using the Hughes protocol, the transaction proceeds as follows. The host and the cryptographic key share a common prime modulus P and generator G, similar to those used in Diffie-Hellman key exchange. The modulus P is typically between 512 and 1024 bits. The host generates a random number Y and computes $Y' = G^Y \bmod P$. The host then requests a secret key

transfer from the cryptographic key and sends Y' as part of the request. The host also calculates a multiplicative inverse Y^{-1} so that $Y^{*}Y^{-1} = 1 \bmod P$.

The cryptographic key generates a secret random number X and sends $Z = (Y')^X \bmod P$ to the host. Since $Y' = G^Y \bmod P$, this means that $Z = (Y')^X \bmod P = G^{XY} \bmod P$. The cryptographic key also computes $K = G^X \bmod P$, but does not send it.

The host then computes $Z^{Y^{-1}} \bmod P$. That is the same as $K = G^X \bmod P$, and K is now a secret key shared between the cryptographic key and the host. The cryptographic key can now use K to encrypt a stored secret. Alternatively, a few calculations could be saved by letting K be the secret key needed by the host. In this case, X would be reused in different sessions, so there would be no need for the cryptographic key to compute $G^X \bmod P$ every time.

Another suitable technique is the RSA public key cipher described in U.S. Patent 4,405,829, the disclosure of which is incorporated herein by reference. That approach is desirable in that it would require fewer computations by the cryptographic key, assuming a low public exponent. However, its use might require the payment of license fees until the patent expires.

For high security applications, the cryptographic key can be provided with a keypad (not shown) for entry of a PIN or other identifying data which is known only to the user. That data can be combined with data stored in the non-volatile memory of the key to provide the secret key which is used in the various protocols. The requirement for the user to enter a PIN prevents unauthorized users from accessing the host with a stolen cryptographic key. For even greater security, the cryptographic key can be programmed to erase the data stored in its internal non-volatile memory if too many incorrect PIN's are entered, or if hardware tampering is detected. Entering the PIN through

the cryptographic key rather than through the host avoids sending secret information over networks which may not be secure.

For all of the cryptographic variable or key transmission techniques discussed above, the transmitted message can be authenticated with digital signatures, or other means, if desired.

In addition to authenticating users to a host, the cryptographic key can also be used for authenticating hosts to a user using the techniques discussed above. This assures a user accessing a remote host through a network that no intruder has tampered with the network and substituted his own computer for the real host. A visual indication as to the success or failure of the authentication protocol is provided by the LED in the cryptographic key.

It is apparent from the foregoing that a new and improved system and method have been provided for controlling access to a system to which access is limited. While only certain presently preferred embodiments have been described in detail, as will be apparent to those familiar with the art, certain changes and modifications can be made without departing from the scope of the invention as defined by the following claims.

CLAIMS

1. In a system for controlling access to a host: a cryptographic key adapted to be carried by a person seeking access to the host, wireless communication means for transmitting information between the key and the host when the key is held in proximity with a transceiver connected to the host, means included in the key for encrypting information for transmission to the host, and means included in the host for decrypting the information from the key and processing the decrypted information to determine whether access to the host is authorized.

2. The system of Claim 1 wherein the wireless communication means comprises infrared transceivers included in the host and in the key.

3. The system of Claim 1 wherein the means for encrypting information includes a microprocessor.

4. The system of Claim 1 wherein the means for encrypting information includes a private encryption code in the cryptographic key.

5. The system of Claim 1 wherein the host comprises a computer, and the means for decrypting the information and processing the decrypted information comprises a microprocessor within the computer.

6. In a method of verifying authorization to access a host, the steps of: storing an encryption code in a cryptographic key which can be carried by a person desiring access to the host, bringing the key into proximity with a wireless transceiver connected to the host, transmitting information over a wireless communication link between the transceiver and the key, encrypting information transmitted from the key to the transceiver in accordance with the encryption code in the key, decrypting the information received by the host,

and processing the decrypted information to determine whether access to the host is authorized.

7. A cryptographic key for obtaining access to a host to which access is limited, comprising a body of a size suitable for attachment to a conventional key chain, a microprocessor within the body, means within the body for storing a cryptographic code, means programming the microprocessor to encrypt information in accordance with the stored code, and transceiver means carried by the body for transmitting encrypted information from the key to the host over a wireless communication link.

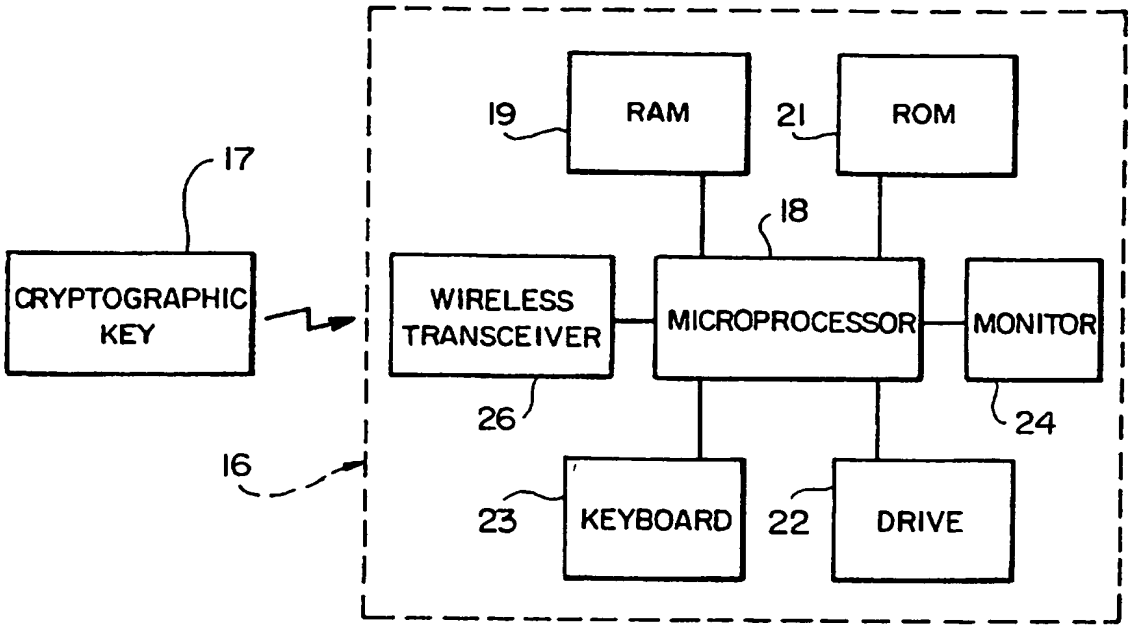

19
RAM
21
ROM
17
18
CRYPTOGRAPHIC KEY
WIRELESS TRANSCEIVER
MICROPROCESSOR
MONITOR
26
24
16
23
KEYBOARD
22
DRIVE

FIG_1

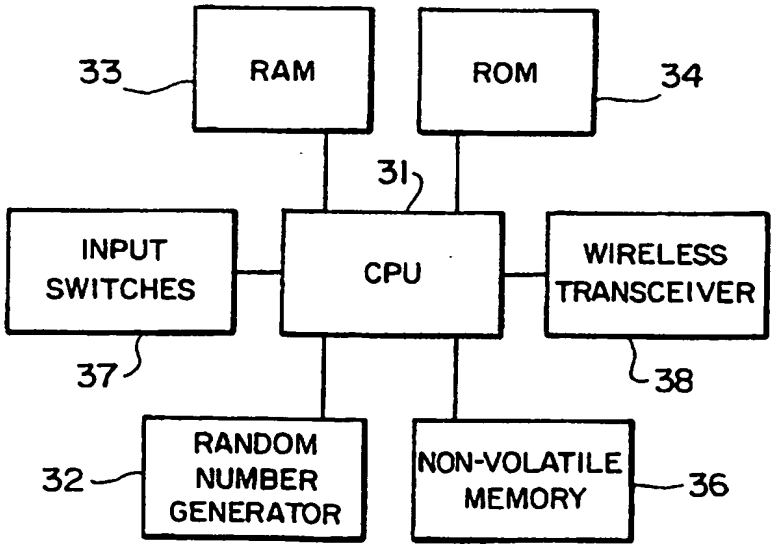

33
RAM
ROM
34
31
INPUT SWITCHES
CPU
WIRELESS TRANSCEIVER
37
38
32
RANDOM NUMBER GENERATOR
NON-VOLATILE MEMORY
36

FIG_2

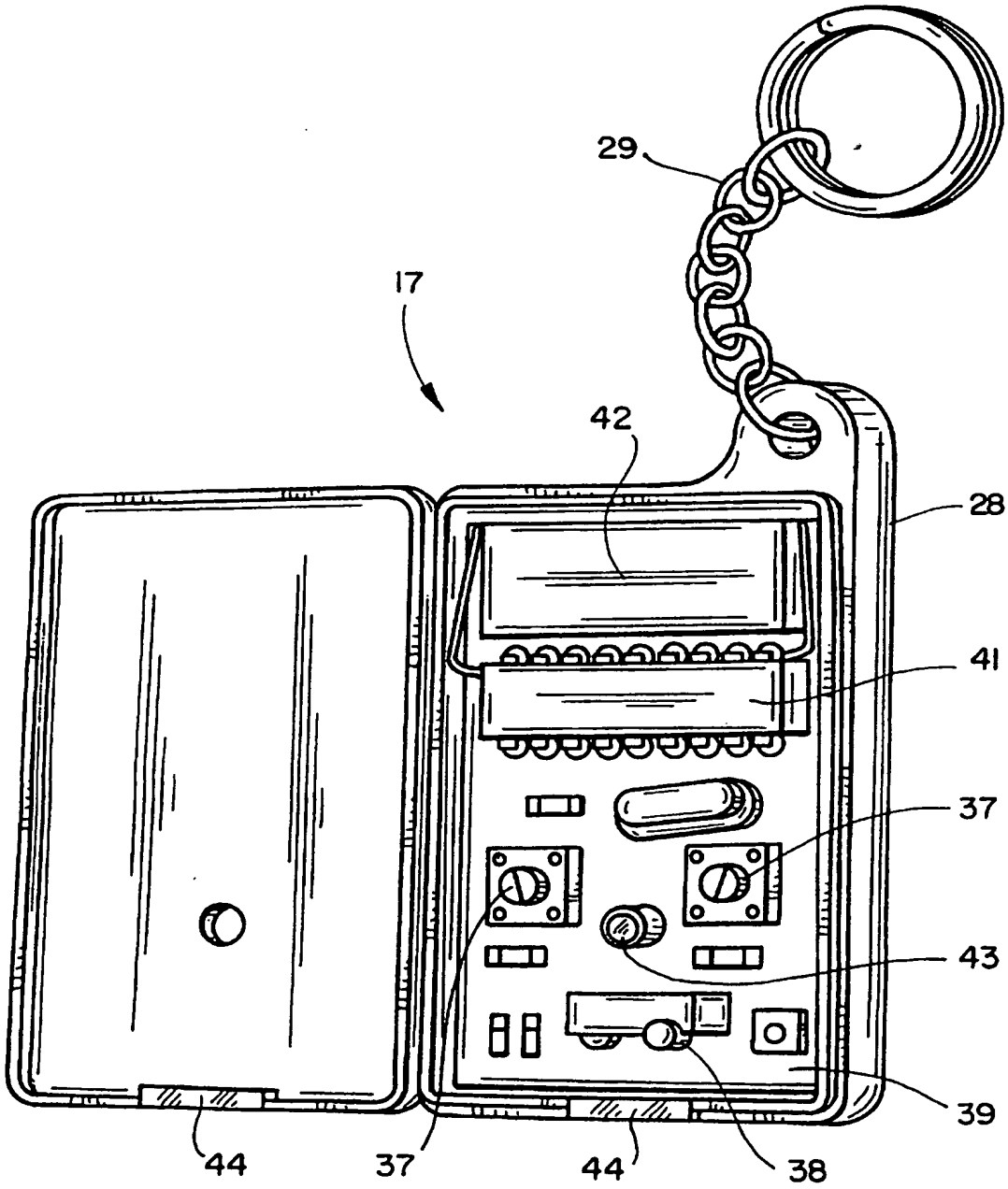


FIG_3

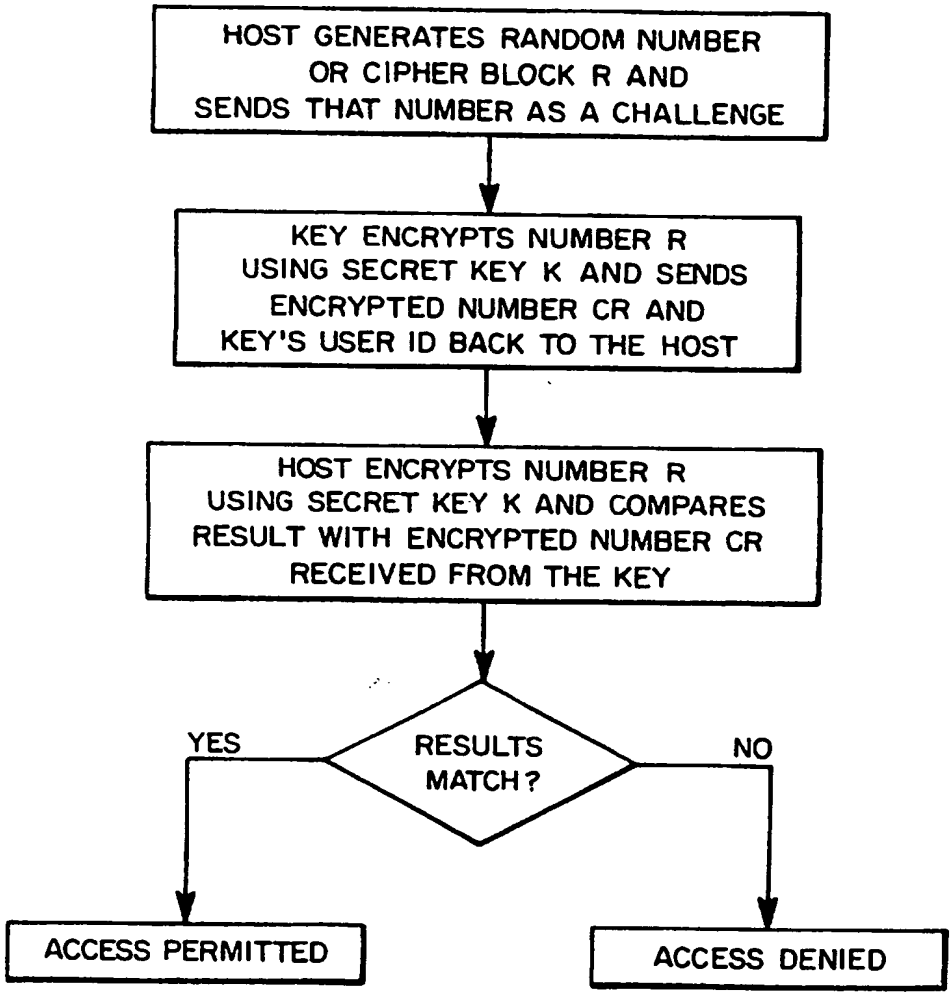

HOST GENERATES RANDOM NUMBER OR CIPHER BLOCK R AND SENDS THAT NUMBER AS A CHALLENGE
KEY ENCRYPTS NUMBER R USING SECRET KEY K AND SENDS ENCRYPTED NUMBER CR AND KEY'S USER ID BACK TO THE HOST
HOST ENCRYPTS NUMBER R USING SECRET KEY K AND COMPARES RESULT WITH ENCRYPTED NUMBER CR RECEIVED FROM THE KEY
RESULTS MATCH?
YES
NO
ACCESS PERMITTED
ACCESS DENIED

FIG_4

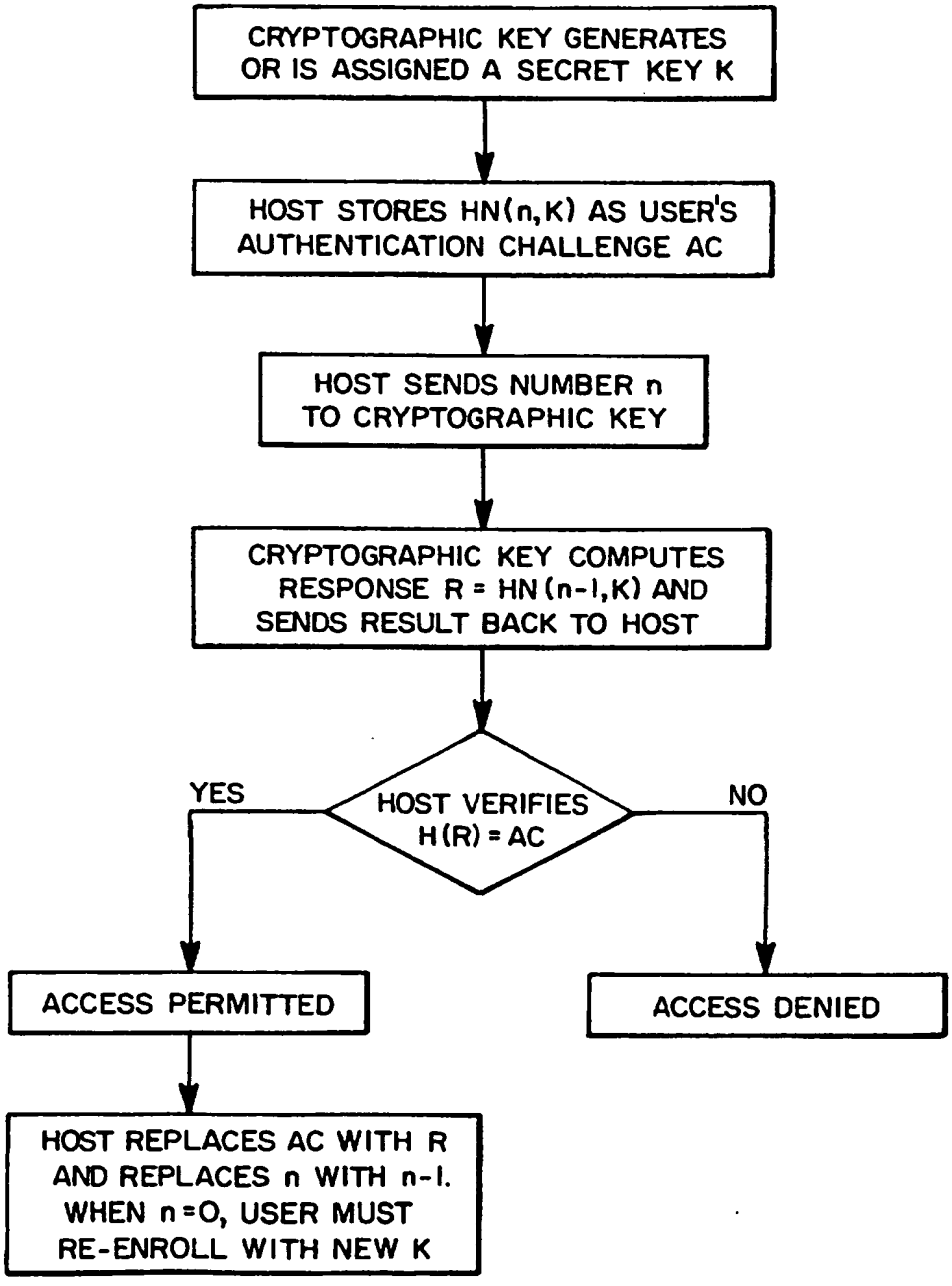

CRYPTOGRAPHIC KEY GENERATES OR IS ASSIGNED A SECRET KEY K
HOST STORES HN(n,K) AS USER'S AUTHENTICATION CHALLENGE AC
HOST SENDS NUMBER n TO CRYPTOGRAPHIC KEY
CRYPTOGRAPHIC KEY COMPUTES RESPONSE R = HN(n-1,K) AND SENDS RESULT BACK TO HOST
HOST VERIFIES H(R) = AC
YES
NO
ACCESS PERMITTED
ACCESS DENIED
HOST REPLACES AC WITH R AND REPLACES n WITH n-1. WHEN n=0, USER MUST RE-ENROLL WITH NEW K

FIG_5

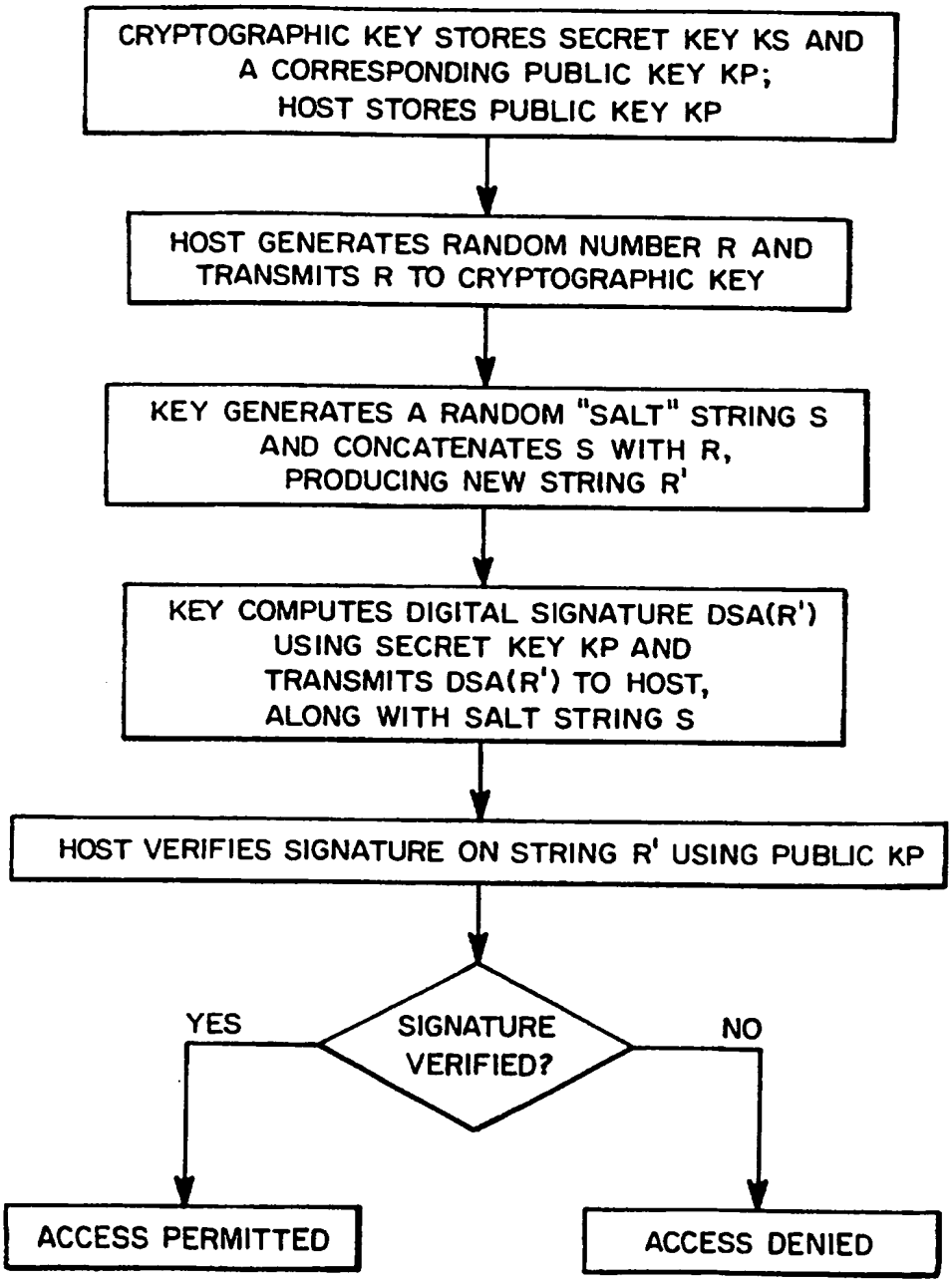

CRYPTOGRAPHIC KEY STORES SECRET KEY KS AND A CORRESPONDING PUBLIC KEY KP; HOST STORES PUBLIC KEY KP
HOST GENERATES RANDOM NUMBER R AND TRANSMITS R TO CRYPTOGRAPHIC KEY
KEY GENERATES A RANDOM "SALT" STRING S AND CONCATENATES S WITH R, PRODUCING NEW STRING R'
KEY COMPUTES DIGITAL SIGNATURE DSA(R') USING SECRET KEY KP AND TRANSMITS DSA(R') TO HOST, ALONG WITH SALT STRING S
HOST VERIFIES SIGNATURE ON STRING R' USING PUBLIC KP
SIGNATURE VERIFIED?
YES
NO
ACCESS PERMITTED
ACCESS DENIED

FIG_6

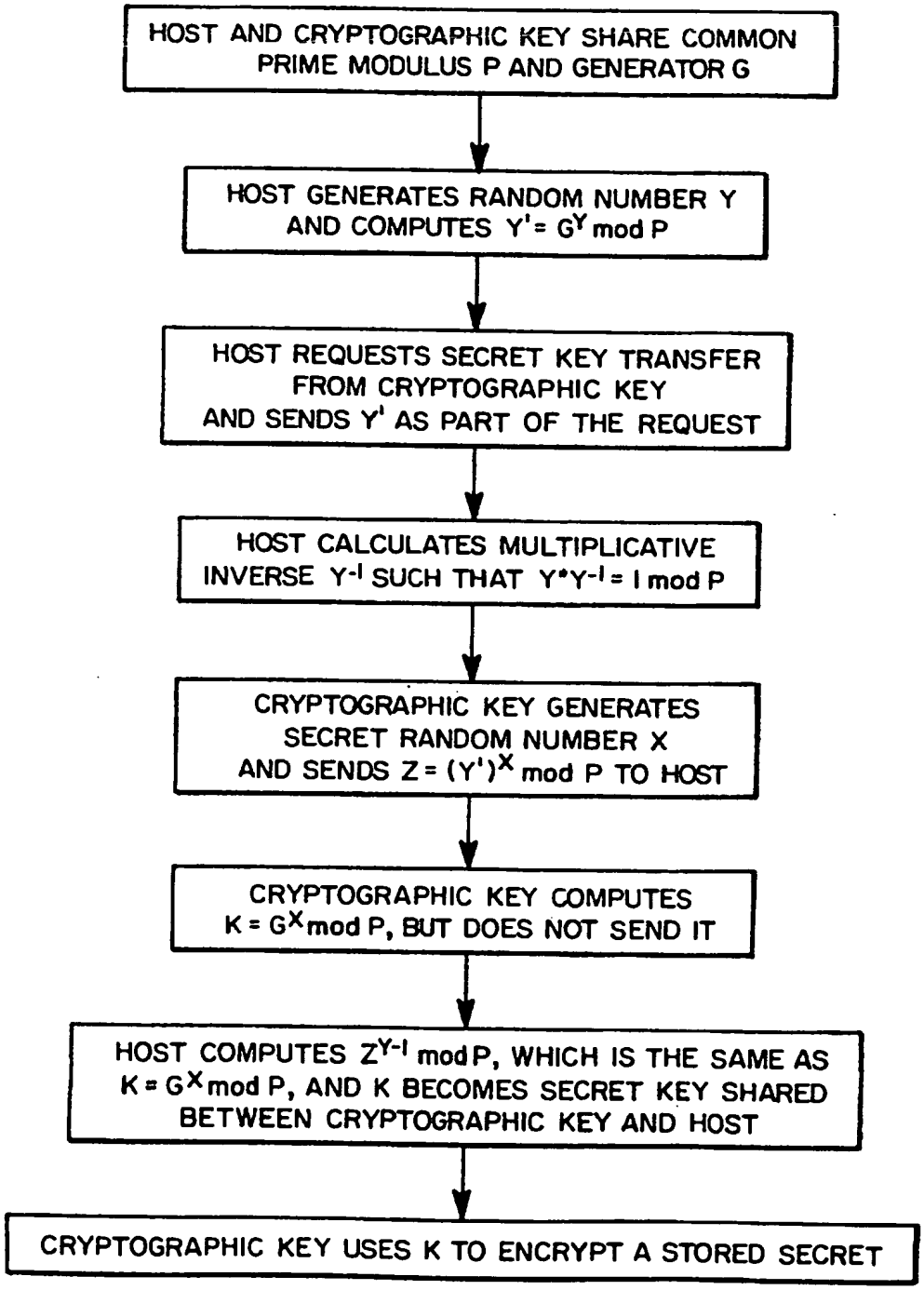

HOST AND CRYPTOGRAPHIC KEY SHARE COMMON PRIME MODULUS P AND GENERATOR G
HOST GENERATES RANDOM NUMBER Y AND COMPUTES Y' = G^Y mod P
HOST REQUESTS SECRET KEY TRANSFER FROM CRYPTOGRAPHIC KEY AND SENDS Y' AS PART OF THE REQUEST
HOST CALCULATES MULTIPLICATIVE INVERSE Y^-1 SUCH THAT Y*Y^-1 = 1 mod P
CRYPTOGRAPHIC KEY GENERATES SECRET RANDOM NUMBER X AND SENDS Z = (Y')^X mod P TO HOST
CRYPTOGRAPHIC KEY COMPUTES K = G^X mod P, BUT DOES NOT SEND IT
HOST COMPUTES Z^Y-1 mod P, WHICH IS THE SAME AS K = G^X mod P, AND K BECOMES SECRET KEY SHARED BETWEEN CRYPTOGRAPHIC KEY AND HOST
CRYPTOGRAPHIC KEY USES K TO ENCRYPT A STORED SECRET

FIG_7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/12840

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00
US CL :380/25
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/25, 21, 23, 24, 44, 46, 49, 50; 340/825.31, 825.34; 235/379, 380

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,800,590 A (VAUGHAN) 24 January 1989, see Abstract.	1-7
A	US 5,377,269 A (HEPTIG et al.) 27 December 1994, see Abstract.	1-7
A	US 5,402,492 A (GOODMAN et al.) 28 March 1995, see Abstract.	1-7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 30 SEPTEMBER 1997	Date of mailing of the international search report 14 JAN 1996
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer BERNARR EARL GREGORY Telephone No. (703) 306-4153

Form PCT/ISA/210 (second sheet)(July 1992)*